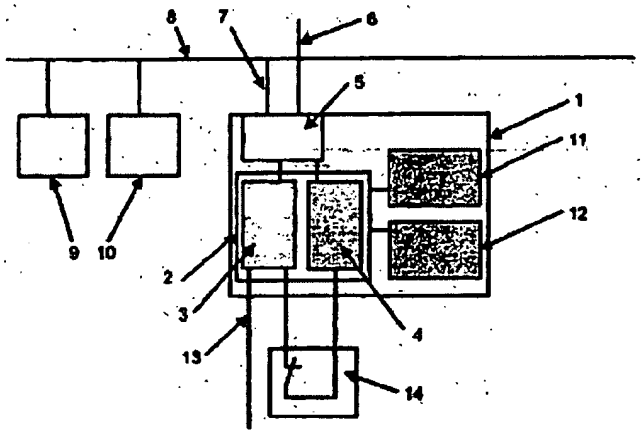
Module for control of safety critical cycles in the control of machines and plant has redundant hardware

Patent number:	DE10025085
Publication date:	2001-12-06
Inventor:	WRATIL PETER (DE)
Applicant:	WRATIL PETER (DE)
Classification:	
- international:	G05B9/03; G05B19/048
- european:	G05B9/03; G05B19/048
Application number:	DE20001025085 20000520
Priority number(s):	DE20001025085 20000520

Abstract of **DE10025085**

The control of safety critical processes of machines has a module (1) with a fault tolerant or two channel structure in which there are redundant hardware stages (3,4) that contain diverse software. Failures or faults are identified and actions initiated for prevention of erroneous machine operations. This uses a control program in memory (11) loaded over an interface (6).



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 25 085 A 1**

(51) Int. Cl.[7]:
G 05 B 9/03
G 05 B 19/048

(21) Aktenzeichen: 100 25 085.8
(22) Anmeldetag: 20. 5. 2000
(43) Offenlegungstag: 6. 12. 2001

D1

DE 100 25 085 A 1

(71) Anmelder:
Wratil, Peter, Dr., 21224 Rosengarten, DE

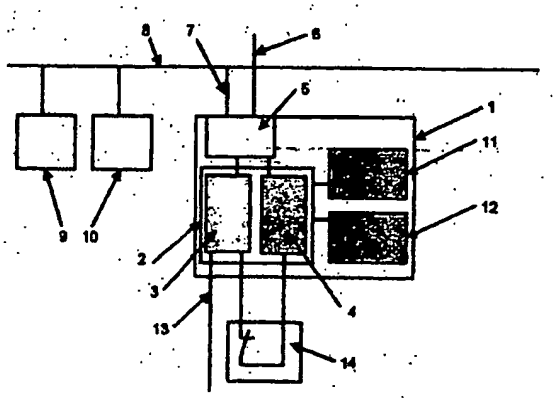
(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Modul zur Steuerung oder Regelung von sicherheitsrelevanten Vorgängen oder Abläufen für den Betrieb von Maschinen oder Anlagen

(57) Es wird ein elektronisches Modul (1) beschrieben, dass sich zur Steuerung oder Regelung von Maschinen oder Anlagen eignet. Das Modul ist intern fehlertolerant aufgebaut und damit in der Lage, mögliche Hard- oder Softwarefehler sicher zu erkennen und zu beherrschen. Die Funktion des Moduls wird über ein Programm vorgegeben, welches sich über eine serielle Schnittstelle (6) oder ein lokales Netzwerk (7) in das Modul laden lässt. Bei Verwaltung eines sicheren Datennetzes (8) können auch Daten oder Zustände von anderen Modulen (9, 10) ausgetauscht werden. Damit wird es mit diesem Modul möglich, sowohl lokale als auch globale Intelligenz - zusammen mit anderen Modulen - als Steuerungs- oder Regelungssystem zu entwickeln.



DE 100 25 085 A 1

[0013] Gleichfalls sind alle internen Zusatzeinrichtungen (wie der Programmspeicher, 11, der Parameterspeicher, 12) entweder doppelt ausgelegt, oder sie werden regelmäßig vollständig auf Richtigkeit überprüft. Das gilt auch für die Eingabe der Daten von der externen Peripherie. Hier lässt sich beispielsweise ein externer Kontakt (14) abfragen, der über spezielle Signalpegel versorgt wird, die ihrerseits ein Signalmuster enthalten. Kurzschlüsse oder nicht erlaubte Verbindungen sind daher schnell erkennbar.

[0014] Vollkommen neu ist die Art der Programmverarbeitung im Modul (1) selbst, oder in einem Verbund von Modulen (1, 9, 10). Jedes dieser Module erhält ein Sicherheitsprogramm, welches im Programmspeicher (11) abgelegt wird. Zusätzlich befindet sich im Parameterspeicher (12) ein Datensatz, der die Funktion des Moduls (1) vorschreibt (z. B. Reaktionszeit, Teilnehmeradresse, Konfiguration des gesamten Bussystems, Zustand anderer Teilnehmer, usw.). Wenn das Modul selbst innerhalb einer Sicherheitsfunktion lokal alle Ein- und Ausgabegrößen für die vollständige Verarbeitung von der angeschlossenen Peripherie (z. B. 13, 14) erhält, so kann die Sicherheitsfunktion ohne das Hinzufügen zusätzlicher Daten ausgeführt werden. Sofern jedoch zur vollständiger Berechnung noch weitere Größen fehlen, werden ausschließlich diese über das Bussystem (8) angefordert. Die weiteren Module (9, 10) senden dann die gewünschten Größen und erhalten ebenfalls alle Daten, so dass sie selbst ihre Funktion erfüllen können.

[0015] Durch dieses Verfahren können an einem Bussystem (8) sowohl autarke Sicherheitsmodule (mit lokaler Sicherheitsfunktion) als auch vernetzte Sicherheitsmodule entstehen, die gemeinsam zu einer komplexen Sicherheitsfunktion beitragen. Im letzteren Fall entsteht ein Sicherheitsverbund mit verteilter Intelligenz.

[0016] Das Bild (Fig. 2) zeigt, wie sich der interne Ablauf zur Verarbeitung im Rahmen einer verteilten Sicherheitsfunktion gestaltet. Jedes Modul (1) erhält ein Programm, das sich nach den angeschlossenen Ausgängen innerhalb des Moduls orientiert. Die notwendige logische Funktion des Ausgangs (7) wird im Programmspeicher abgelegt und von den beiden Verarbeitungseinheiten durchgeführt. Wenn alle notwendigen Eingangsgrößen (zur Kalkulation der geforderten Ausgangsgröße) bereits intern zur Verfügung stehen (über die interne Ein- und Ausgabeeinheit im Modul, 6), so gelingt die autarke Verarbeitung der Sicherheitsfunktion.

[0017] In dem Fall, dass man zur Erfüllung der gewünschten Sicherheitsfunktion externe Eingangsgrößen braucht (z. B. von den Modulen 2 und 3), so werden diese Daten (5) entweder zyklisch oder auf Anforderung über das Bussystem (4) übertragen. Es versteht sich von selbst, dass die Datenübertragung ebenfalls gesichert erfolgen muss, damit man eine Datenverfälschung ausschließen kann.

[0018] Jede übertragene Eingangsfunktion legt das Modul (1) in einem Datenspeicher (Parameterspeicher) ab. Dabei wird sowohl der aktuelle Inhalt als auch die Zeit (oder ein entsprechender Zeitwert) festgehalten (8,10). Der Zeitwert wird durch eine Uhr oder einen Timer (9) zusätzlich zum Datum (8) als Information hinzugefügt (10).

[0019] Mit den Inhalten aus dem Parameterspeicher kann nun die Verarbeitungslogik (oder beide Einheiten) die gewünschte Funktion (7) erfüllen und den angeschlossenen Ausgang über die Peripherieeinheit (6) bedienen.

[0020] Da in der Sicherheitstechnik jeder Ablauf mit einer festen Reaktionszeit erfolgen muss, enthält jedes Datum (eines externen Moduls 2, 3) auch die aktuelle Zeit der Ablage oder der Versendung. Wenn es innerhalb der gewünschten Reaktionszeit nicht gelingt, ein neues Datum zu der entsprechenden Einheit zu übertragen, so wird von dem Modul (1, 2,3) ein sicherer Zustand eingeleitet. Dieser besteht in der Regel darin, den Ausgang zu deaktivieren.

[0021] Durch diese Maßnahme wird gewährleistet, dass bei einem Defekt einer externen Einheit oder bei Ausfall des Bussystems, stets ein sicherer Zustand erreicht wird. Das Verfahren hat zudem noch den Vorteil, dass nur diejenigen Daten über den Bus übertragen werden, die nicht in den Einheiten selbst vorliegen. Die Datenrate und die damit verbundene Auslastung des Bussystems (4) können somit gering gehalten werden.

[0022] Zur Verteilung der programmierbaren Funktionen wird ein Übersetzer (Compiler) benötigt, der die logischen Pfade entsprechend der gewünschten Ausgangsfunktion berechnet. Hierdurch entstehen Programmteile, die sich in jedes Modul herunterladen lassen. Das Verfahren der Blockbildung und der Dezentralisierung ist bereits in der Norm IEC 1131-3 beschrieben und kann bei der Programmierung des hier vorgestellten System der verteilten Sicherheit angewendet werden.

BEZUGSZEICHENLISTE

Abb. 1

1 Modul
2 2kanalige fehlertolerante Struktur (eventuell mit redundanter Hard- und diversitärer Software)
3 Verarbeitungslogik (Kanal 1)
4 Verarbeitungslogik (Kanal 2)
5 Interface (zur Kommunikation mit einem lokalen Netz oder einer seriellen Schnittstelle)
6 Serielle Schnittstelle (Option)
7 Anschluss an ein lokales Netzwerk
8 Lokales Netzwerk
9 Weiteres Modul am Netzwerk
10 Weiteres Modul am Netzwerk
11 Programmspeicher zur Ablage des Programms (zur Erfüllung der Sicherheitsfunktion)
12 Parameterspeicher (zur Ablage der Konfiguration, Diagnose, Status und der Zustände im Modul und im Netzwerk)
13 Ein- oder Ausgabekanal zur Steuerung oder Regelung
14 Beispiel eines Anschlusses extern verdrahteter Sicherheitseinheiten

Abb. 2

Legende:
1 Modul
2 Weiteres Modul
3 Weiteres Modul
4 Datenübertragung über lokales Netzwerk
5 Datum, Ein- oder Ausgangswert von fremden Modul
6 Ein- und Ausgabeeinheit im eigenen Modul
7 Logik zur Berechnung der Daten und Ausgabefunktion
8 Dateninhalt (im Speicher) von externem Modul
9 Interne Uhr
10 Zeitwert bei Dateneingang vom Netzwerk

Patentansprüche

1. Modul (Fig. 1: 1) zur Steuerung oder Regelung von sicherheitsrelevanten Vorgängen oder Abläufen für den Betrieb von Maschinen oder Anlagen, **dadurch gekennzeichnet**, dass das Modul (Fig. 1: 1) aus einer fehlertoleraten oder einer vergleichbaren 2kanaligen Struktur (Fig. 1: 2) besteht, die eine redundante Hardware (Fig. 1: 3, 4) und eine diversitäre Software enthält, die in dem Modul (Fig. 1: 1) hinterlegt wird, damit sowohl Bauteilausfälle oder Störungen als auch systematische Fehler erkannt und sicher beherrscht werden, sowie Ein- und Ausgabekanäle zur Verfügung stellt (Fig. 1: 13), damit der sichere Betrieb externer Geräte

ermöglicht wird, deren Funktion oder Ablauf durch eine Programm vorgegeben wird, das sich im Programmspeicher (Fig. 1: 11) befindet, das sich mittels einer seriellen Schnittstelle (Fig. 1: 6) oder eines lokalen Netzes (Fig. 1: 7) über ein Interface (Fig. 1: 5) in das Modul (Fig. 1: 1) laden lässt, damit das Modul sowohl lokale Intelligenz als programmierbare autarke Einheit, als auch globale Intelligenz im Zusammenwirken mit anderen ähnlich oder identisch aufgebauten Modulen (Fig. 1: 9, 10) über ein geeignetes Netzwerk (Fig. 1: 8) oder einen Datenübertragungskanal entwikkeln kann.

2. Modul nach dem Anspruch 1, dadurch gekennzeichnet, dass die Programmierung über Standardsprachen möglich ist, die den sicheren Ablauf und die Funktion von Maschinen oder Anlagen beschreiben oder darstellen, und dass dieses Programm in einem Programmspeicher (Fig. 1: 11) hinterlegt wird.

3. Modul nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, dass ein komplexes Sicherheitsprogramm für eine Maschine oder Anlage sich derart aufteilen oder gliedern lässt, dass sich Teile in mehrere Module unterbringen lassen und damit das gesamte Gefüge eine vollständiges Sicherheitssystem darstellt.

4. Modul nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass sich Zustände, Daten, Ein- und Ausgangswerte von anderen Modulen übertragen lassen, damit man gesicherte Funktionen auch bei Überwindung größerer Distanzen oder unter Verwendung zahlreicher peripherer Größen erreichen kann.

5. Modul nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, dass Status- und Diagnosefunktionen zur Verfügung gestellt werden, die in einem Parameterspeicher liegen (Fig. 1: 12), damit man über den Ablauf oder die Funktion der Maschine oder Anlage weiträumig informiert ist.

6. Modul nach den Ansprüchen 1 bis 5, dadurch gekennzeichnet, dass eine laufende interne Kontrolle durchgeführt wird, damit mögliche Fehler in der angeschlossenen Peripherie als auch im Modul selbst erkannt und übermittelt werden.

7. Modul nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, dass sich das Programm zur Erfüllung der Sicherheit auch nachträglich oder sogar während des Betriebs laden lässt, und in den Programmspeicher (Fig. 1: 11) gelangt.

8. Modul nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, dass ein interner Parameterspeicher (Fig. 1: 12) existiert, dessen Inhalt für die Funktion, die Arbeitsweise und den Zustand aller internen Größen, sowie die Ein- und Ausgänge verantwortlich ist.

9. Modul nach den Ansprüchen 1 bis 8, dadurch gekennzeichnet, dass die Ein- und Ausgänge auch verdrahtete Sicherheitsvorrichtungen (Fig. 1: 14) betreiben können und die entsprechenden Testmuster zur Fehlererkennung von Drahtbrüchen oder Kurzschlüssen zur Verfügung stellen können.

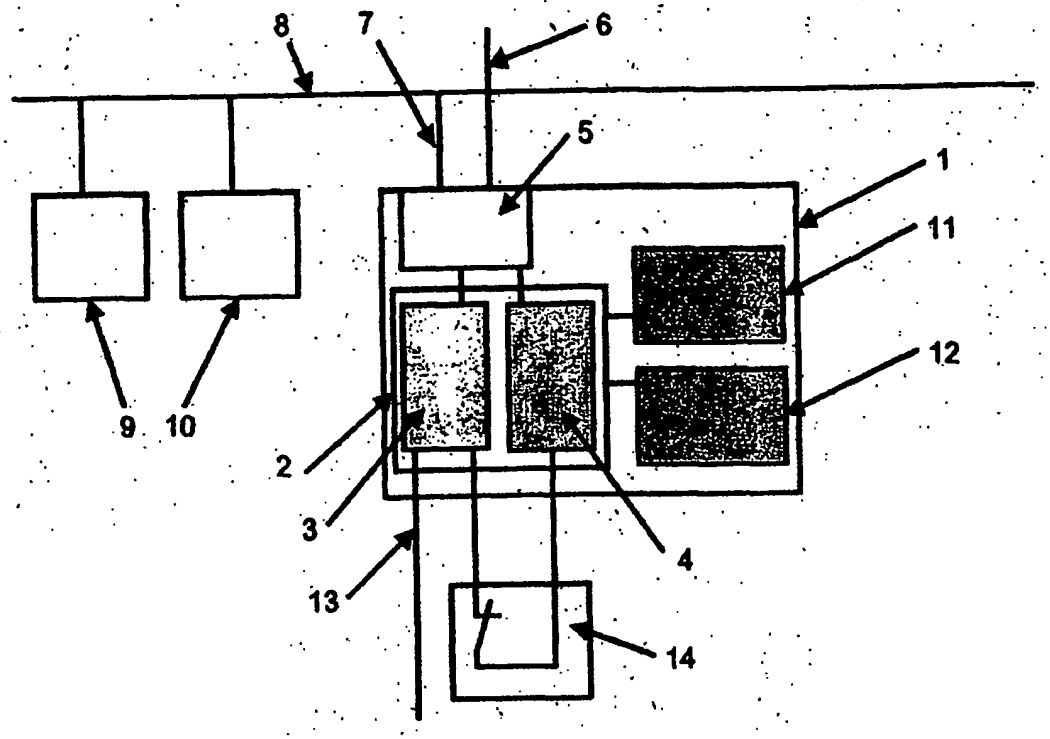
10. Modul nach den Ansprüchen 1 bis 9, dadurch gekennzeichnet, dass der Datentransport (Fig. 2: 4) zusätzlicher Ein- und Ausgabegrößen fremder Module über ein Uhr (Fig. 2: 9) überwacht wird. Hierdurch wird das Modul in einen sicheren Zustand geschaltet, wenn über einen definierbaren Zeitraum keine Antwort einer, für die interne Funktion des jeweiligen Moduls notwendige, Größe übertragen wird. Hierdurch ist eine sicherheitsgerichtete Kontrolle des gesamtes Netzwerkes gegeben.

11. Modul nach den Ansprüchen 1 bis 10, dadurch gekennzeichnet, dass die Daten, Ein- oder Ausgangsgrößen fremder Module über ein sicherheitsgerichtes Datennetz oder ein lokales Netzwerk (Fig. 2: 4) mit Sicherheitsarchitektur übertragen werden.

Hierzu 2 Seite(n) Zeichnungen

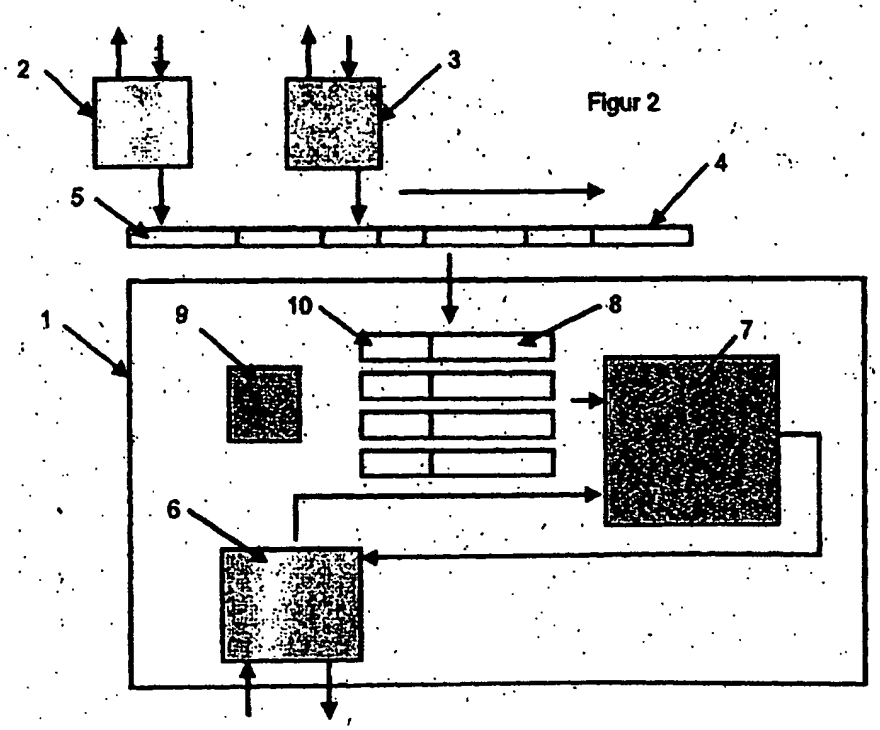
Nummer: DE 100 25 085 A1
Int. Cl.[7]: G 05 B 9/03
Offenlegungstag: 6. Dezember 2001

Figur 1



Nummer: DE 100 25 035 A1
Int. Cl.[7]: G 05 B 9/03
Offenlegungstag: 6. Dezember 2001

Abbildung 2



Figur 2